IN THE CLAIMS

1. (Withdrawn) A tamper-resistant processing method comprising the steps of:

(1) storing a secret key index x corresponding to a public key of RSA (e, N; modulus N being a product of 2 primes p and q) in a storage device;

(2) inputting a ciphertext Y through an input means;

(3) calculating yp, a remainder of y, based on a modulus of either P or its multiple and yq, a remainder of y, based on a modulus of either Q or its multiple; and

(4) when calculating Cp which is a remainder of yp^xp based on a modulus of either of p or its multiple and calculating Cq which is a remainder of yq^xq based on a modulus of either q or its multiple, where a remainder of x based on a modulus of either of p-1 or its multiple is put as xp, and a remainder of x based on a modulus of either q-1 or its multiple is put as xq,

(4a) deciding which process (4b) or (4c) is to be executed for each processing of a bit block which is a bit string of at least 1 bit composing xp, xq;

(4b) executing a predetermined modular exponentiation calculation on said bit block to be processed by xp and for storing the calculation result in the storage device;

(4c) executing a predetermined modular exponentiation calculation on said bit block to be processed by xq and for storing the calculation result in the storage device;

(5) calculating RSA decryption calculation, $y^{A}x \bmod N$ based on a difference between Cp and Cq, when the calculation of Cp about the whole of xp, and the calculation of Cq about the whole of xq are finished; and

(6) outputting the result of said RSA decryption calculation.

2. (Withdrawn) A tamper-resistant processing method of claim 1 wherein for said yp, yq, xp and xq, calculation be made as: yp = y mod p, yq = y mod q, xp = x mod (p-1), xq = x mod (q-1).

3. (Withdrawn) A tamper-resistant processing method of claim 1 wherein which one of said steps (4b) and (4c) is to be processed is determined with the use of a generated random number.

4. (Withdrawn) A tamper-resistant processing method of claim 1 wherein the process of said step (4a) is applied to a part of bit patterns of said xp or xq, and for a remaining part of the bit patterns, after said either one of step (4b) or (4c) is processed, another one is processed.

5. (Currently amended) A tamper-resistant processing method comprising the steps of:

[[(1)]] (a) deciding which step is to be selected out of the following steps [[(2)]] (b) and [[(3)]] (c) for each processing of one operation unit;

[[(2)]] (b) after transferring one operation unit in the bit pattern of data A in a memory in order of its bit sequence to a first register R1, transferring one operation unit in the bit pattern of data B in the memory in order of its bit sequence to a second register R2;

[[(3)]] (c) after transferring one operation unit in the bit pattern of said data B in order of its bit sequence to said second register R2, transferring one operation unit in the bit pattern in said data A in order of its bit sequence to said first register R1;

[[(4)]] (d) executing a predetermined arithmetic operation on the contents of said first register R1 and the contents of said second register R2;

[[(5)]] (e) storing the result of said arithmetic operation in the memory,

[[(6)]] (f) repeating the steps from [[(1)]] (a) through [[(5)]] (e) until said arithmetic operation for said data A and said data B is finished.

6. (Currently amended) A tamper-resistant processing method comprising the steps of:

[[(1)]] (a) deciding which step is to be selected out of the following steps [[(2)]] (b) and [[(3)]] (c) for each processing of one operation unit;

[[(2)]] (b) after transferring one operation unit of data A in a memory in order of its bit sequence to a first register R1, transferring one operation unit of data B in the memory in order of its bit sequence to a second register R2;

[[(3)]] (c) after transferring said one operation unit of the data A in order of its bit sequence to said second register R2, transferring said one operation unit of the data B in order of its bit sequence to said first register R1;

[[(4)]] (d) executing a predetermined arithmetic operation on the contents of said first register R1 and on the contents of said second register R2;

[[(5)]] (e) storing the result of said arithmetic operation in the memory;

[[(6)]] (f) repeating the steps from [[(1)]] (a) through [[(5)]] (e) until said arithmetic operation on said data A and said data B is finished.

7. (Currently amended) A tamper-resistant processing method of claim 6 wherein which one out of said steps [[(2)]] (b) and [[(3)]] (c) is to be processed is determined with the use of a generated random number.

8. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic sum.

9. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic product.

10. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is any one of the logical sum OR, logical product AND, and exclusive logical sum EXOR.

11. (Currently amended) A tamper-resistant processing method comprising the steps of:

[[(1)]] (a) selecting any one of unprocessed one operation unit in a bit pattern of data A in a memory;

[[(2)]] (b) transferring said one operation unit of said data A selected to a first register R1;

[[(3)]] (c) transferring one operation unit in a bit pattern of data B in the memory corresponding to said one operation unit of said data A selected to a second register R2;

[[(4)]] (d) executing a predetermined arithmetic operation for the contents of said first register R1 and the contents of said second resister R2;

[[(5)]] (e) storing a result of said arithmetic operation in the memory;

[[(6)]] (f) repeating the steps from (1) through (5) until said arithmetic operation is finished on said data A and said data B.

12. (Original) A tamper-resistant processing method of claim 11 wherein corresponding to a generated random number, said unprocessed one operation unit is selected.

13. (Original) A tamper-resistant processing method of claim 11 wherein said predetermined arithmetic operation is any one of logical sum OR, logical product AND, and exclusive logical sum EXOR.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.